Remarks

The Office Action mailed August 9, 2007 has been carefully reviewed and the following remarks have been made in consequence thereof.

Claims 1-9, and 11-64 are now pending in this application. Claims 1-62 are rejected. Claim 10 is canceled without prejudice, waiver, or disclaimer. Claims 1-9 and 11-62 are amended. Claims 63 and 64 are newly added. No new matter has been added. A fee calculation sheet is submitted herewith for the newly added claims.

In accordance with 37 C.F.R. 1.136(a), a two-month extension of time is submitted herewith to extend the due date of the response to the Office Action dated August 9, 2007 for the above-identified patent application from November 9, 2007 through and including December 9, 2007. In accordance with 37 C.F.R. §1.17(a)(2), authorization to charge a deposit account in the amount of $230.00 to cover this extension of time request also is submitted herewith.

The rejection to Claims 1, 26, 27, 28, 50, 51, and 62 under 35 U.S.C. §112, second paragraph is respectfully traversed. Applicant has amended Claims 1, 26, 27, 28, 50, 51, and 62, and respectfully submits that Claims 1, 26, 27, 28, 50, 51, and 62, as amended, particularly point out and distinctly claim the subject matter which Applicant regards as his invention. Accordingly, Applicant respectfully requests that the rejection under 35 U.S.C. §112 be withdrawn.

The objection to Claim 1 is respectfully traversed. Applicant has amended Claim 1. Accordingly, Applicant respectfully requests that the objection to Claim 1 be withdrawn.

The provisional double patenting rejection of Claims 9, 34, 40, 45, 55, and 58 as being unpatentable over Claims 16, 17, and 110 in co-pending U.S. Patent Application Nos. 10/458,858, 10/459,019, 10/459,350, 10/459,349, 10/459,297, and 10/458,844 is respectfully traversed. Claims 9, 34, 40, 45, 55, and 58 are amended by this Amendment. Moreover, Claims 16, 17, and 110 in the co-pending patent applications have not yet issued in a U.S. patent. Applicants will consider filing a terminal disclaimer when the present application is indicated as allowable.

For at least the reasons set forth above, Applicant respectfully requests that the double patenting rejection of Claims 9, 34, 40, 45, 55, and 58 be withdrawn.

The rejection of Claims 9, 34, 40, 45, 55, and 58 under 35 U.S.C. § 103(a) as being unpatentable over Lee (U.S. Patent No. 7,047,561) in view of Zaumen et al. (U.S. Patent No. 7,234,003) is respectfully traversed.

Lee describes a firewall for real-time Internet applications. The firewall includes a packet filter (106) that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks (110 and 120) (column 4, lines 40-43). The packet filter follows predetermined security rules that specify which types of packets to allow to pass and which types of packets to block (column 4, lines 43-45).

Zaumen et al. describe a system that facilitates a direct transfer of data. The system operates by receiving a request at a multiplexer from a controller to transfer the data from a data device to a data terminal (abstract). The multiplexer forwards the request to the data device that has the requested data (abstract). The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device (abstract). The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller (abstract).

Claim 9 recites a security system comprising "a network configured to transport network traffic, wherein said network comprises a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands said hardware processor; said hardware processor comprising: an RDMA mechanism for performing RDMA data transfer; a protocol processing engine to do transport layer protocol processing; a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules; an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols; and a packet classification engine to classify the network traffic, said security system providing multiple protocol layer security in said network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 9. For example, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands the hardware processor, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands the hardware processor. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands the hardware processor, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do

encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. For the reasons set forth above, Claim 9 is submitted to be patentable over Lee in view of Zaumen et al.

Claim 34 recites a security system comprising "a network comprising a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol, said hardware processor comprising an RDMA mechanism for performing RDMA data transfer, said security system providing multiple protocol layer security in said network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 34. For example, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol. Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol. For the reasons set forth above, Claim 34 is submitted to be patentable over Lee in view of Zaumen et al.

Claim 40 recites a security system comprising "a remote direct memory access (RDMA) processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol, said security system providing multiple protocol layer security in said network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 40. For example, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a remote direct memory access (RDMA) processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol. Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest an RDMA processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest an RDMA processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol. For the reasons set forth above, Claim 40 is submitted to be patentable over Lee in view of Zaumen et al.

Claim 45 recites a security system comprising "a storage area network comprising a remote direct memory access (RDMA) capability for performing RDMA data transfers, said security system providing multiple protocol layer security in said storage area network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 45. For example, neither Lee nor

Zaumen et al., considered alone or in combination, describe or suggest a storage area network comprising a remote direct memory access (RDMA) capability for performing RDMA data transfers, the security system providing multiple protocol layer security in the storage area network. Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest a storage area network. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a storage area network comprising a remote direct memory access (RDMA) capability for performing RDMA data transfers, the security system providing multiple protocol layer security in the storage area network. For the reasons set forth above, Claim 45 is submitted to be patentable over Lee in view of Zaumen et al.

Claim 55 recites a security system comprising "a network comprising a hardware processor providing a remote direct memory access (RDMA) capability, said hardware processor comprising: an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing; said security system providing multiple protocol layer security in said network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 55. For example, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest the hardware processor comprising an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing.

Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest the hardware processor comprising an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest the hardware processor comprising an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing. For the reasons set forth above, Claim 55 is submitted to be patentable over Lee in view of Zaumen et al.

Claim 58 recites a security system comprising "a storage area network comprising a hardware processor providing a remote direct memory access (RDMA) capability, said hardware processor comprising an RDMA mechanism for performing RDMA data transfer, said security system providing multiple protocol layer security in said storage area network."

Neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a security system as recited in Claim 58. For example, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a storage area network comprising a hardware processor providing a remote direct memory access (RDMA) capability, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, the security system providing multiple protocol layer security in the storage area network. Rather, Lee describes a firewall that includes a packet filter that examines a plurality of packets at layer 3 and layer 4 to

selectively control flow of data to and from a plurality of networks. Zaumen et al. describe a multiplexer that forwards a request to a data device that has the requested data. The request is received from a controller and the request is for transferring data from the data device to a data terminal. The multiplexer then receives a set of parameters from the data device, including a location of outgoing data within the data device. The multiplexer moves the data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller. A description of the firewall that examines the packets at layers 3 and 4, and the multiplexer that moves data from the data device into an outgoing data stream, thereby removing the necessity of first copying the data into the controller does not describe or suggest a storage area network. Accordingly, neither Lee nor Zaumen et al., considered alone or in combination, describe or suggest a storage area network comprising a hardware processor providing a remote direct memory access (RDMA) capability, said hardware processor comprising an RDMA mechanism for performing RDMA data transfer, the security system providing multiple protocol layer security in said storage area network. For the reasons set forth above, Claim 58 is submitted to be patentable over Lee in view of Zaumen et al.

For at least the reasons set forth above, Applicant respectfully requests that the rejections of Claims 9, 34, 40, 45, 55, and 58 under 35 U.S.C. 103(a) be withdrawn.

Notwithstanding the above, Applicant respectfully submits that the Section 103 rejection of Claims 9, 34, 40, 45, 55, and 58 is not a proper rejection. It appears to the Applicant that the present rejection reflects an impermissible attempt to use the instant claims as a guide or roadmap in formulating the rejection using impermissible hindsight reconstruction of the invention. It is also impermissible to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. The United States Supreme Court has recently expressed concern regarding distortion caused by hindsight bias in an obvious analysis, and notes that "[a] factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of argument reliant upon ex post reasoning." KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 82 USPQ2d at 1397. See also Ex parte Rinkevich, 2007 WL 1552288 (Bd. Pat. App. & Interf. May 29,

2007). Following the Supreme Court's guidance provided in KSR Int'l Co. v. Teleflex Inc. with respect to impermissible hindsight, a person of ordinary skill in the art having common sense at the time of the invention would not have reasonably looked to Lee or Zaumen et al. to solve the problem associated with efficiently communicating data in a manner recited in Claims 9, 34, 40, 45, 55, and 58. Rather, such a suggestion is disclosed only in the present application. For at least this reason alone, Applicant requests that the Section 103 rejection be withdrawn.

Further, the Office Action only offers the conclusory statement that "[i]t would have been obvious to one skilled in the art to implement the RDMA teaching of transfer data into Lee's teaching in order to control the data transfer across network to ensure that authorized data is access through network" to suggest the combination of Lee and Zaumen et al. Obviousness rejections must be supported with "articulated reasoning with some rational underpinning to support the conclusion of obviousness." See KSR International Co. v. Teleflex, Inc., 127 S. Ct. 1727 at 1740-41, 82 USPQ2d at 1396, citing In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). The present rejection does not appear to meet this standard as it reflects no articulated reasoning why the independent or dependent claims are believed to be obvious, but rather is stated in the form of a conclusion of obviousness. Applicant accordingly requests specific explanation and articulation regarding the reasoning and rational underpinning for any obviousness rejection of the claims, or request that the Examiner remove the rejection. It is not believed that adequate reasons why the presently claimed invention is believed to be obvious have been provided on the present record.

For at least the reasons set forth above, Applicant respectfully requests that the rejections of Claims 9, 34, 40, 45, 55, and 58 under 35 U.S.C. 103(a) be withdrawn.

The rejection of Claims 1-9 and 11-62 under 35 U.S.C. § 102(e) as being anticipated by Bruton, III et al. (U.S. Patent No. 7,076,803) is respectfully traversed.

Bruton, III et al. describe an integrated intrusion detection system. The system includes a host (310) that is depicted as taking responsibility for its own intrusion

detection (column 5, lines 52-53). It may be desirable in some situations to continue using a sniffer in front of the host (column 5, lines 54-56). The system further includes a plurality of servers (400a, 400b, 400c) (column 7, lines 42-44). Once an Intrusion Detection System (IDS) policy information is available from a repository (410), the information may be downloaded to one or more of the servers (column 7, lines 42-44). The system also includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer IDS functions (column 10, lines 5-6).

Claim 1 recites a network system comprising "a network configured to transport network traffic, wherein said network comprises a plurality of distributed security systems providing multiple protocol layer security, wherein each of said distributed security systems comprises at least one host processor and said distributed security systems comprise a hardware processor offloading overhead of transport layer protocol processing from said at least one host processor, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said hardware processor comprising: a protocol processing engine to do transport layer protocol processing; a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules; an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols; and a packet classification engine to classify the network traffic."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 1. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor, the hardware processor comprising a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton,

III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor, the hardware processor comprising a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. For the reasons set forth above, Claim 1 is submitted to be patentable over Bruton, III et al.

Claims 3-8, 17, and 19 depend from independent Claim 1. When the recitations of Claims 3-8, 17, and 19 are considered in combination with the recitations of Claim 1, Applicant submits that Claims 3-8, 17, and 19 are patentable over Bruton, III et al.

Claim 2 recites a security system comprising "a storage area network configured to transport storage area network traffic, wherein said storage area network comprises at least one network system, wherein said at least one network system comprises a hardware processor providing transport layer protocol processing, said hardware processor comprising: a storage protocol processing engine to do storage protocol processing; a protocol processing engine to do transport layer protocol processing; a programmable rule-matching engine to analyze the storage area network

traffic for security rule matching or taking actions on matched security rules; an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols; a packet classification engine to classify the storage area network traffic; and a packet processing engine to perform packet processing tasks like header processing or deep packet processing, said security system providing multiple protocol layer security in said storage area network."

Bruton, III et al. do not describe or suggest a security system as recited in Claim 2. For example, Bruton, III et al. do not describe or suggest a storage area network configured to transport storage area network traffic, wherein the storage area network comprises at least one network system, wherein the at least one network system comprises a hardware processor providing transport layer protocol processing, the hardware processor comprising a storage protocol processing engine to do storage protocol processing, a protocol processing engine to do transport layer protocol processing; a programmable rule-matching engine to analyze the storage area network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, a packet classification engine to classify the storage area network traffic, a packet processing engine to perform packet processing tasks like header processing or deep packet processing, the security system providing multiple protocol layer security in the storage area network. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a storage area network. For the reasons set forth above, Claim 2 is submitted to be patentable over Bruton, III et al.

Claims 20-25 depend from independent Claim 2. When the recitations of Claims 20-25 are considered in combination with the recitations of Claim 2, Applicant submits that Claims 20-25 are patentable over Bruton, III et al.

Claims 11-16 and 18 depend from independent Claim 9, which is recited above.

Bruton, III et al. do not describe or suggest a security system as recited in Claim 9. For example, Bruton, III et al. do not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands the hardware processor, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to offload transport layer protocol processing from a host processor that commands the hardware processor, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, a protocol processing engine to do transport layer protocol processing, a programmable rule-matching engine to analyze the network traffic for security rule matching or taking actions on matched security rules, an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols, and a packet classification engine to classify the network traffic. For the reasons set forth above, Claim 9 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 11-16 and 18 are considered in combination with the recitations of Claim 9, Applicant submits that Claims 11-16 and 18 are patentable over Bruton, III et al.

Claims 26 recites a network system comprising "a network configured to transport network traffic, wherein said network comprises a plurality of distributed security systems providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor and said distributed security systems comprise a hardware processor offloading overhead of transport layer protocol processing from said at least one host processor of said distributed security systems, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor; said hardware processor comprising a protocol processing engine to do transport layer protocol processing; a programmable rule-matching to analyze the network traffic for security rule matching or taking actions on matched security rules; or an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols; or a packet classification engine to classify the network traffic; or a packet processing engine to perform packet processing tasks like header processing or deep packet processing or a combination thereof; or a combination of the foregoing."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 26. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor of the distributed security systems, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor of the distributed security systems, wherein the

hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor of the distributed security systems, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. For the reasons set forth above, Claim 26 is submitted to be patentable over Bruton, III et al.

Claim 27 recites a network system comprising "a network comprising a plurality of distributed security systems and one or more networked systems, each of said distributed security systems comprising at least one host processor, and at least one of said distributed security systems comprising a first hardware processor and a second hardware processor configured to offload overhead of a protocol processing stack from said at least one host processor, said distributed network security systems providing a secure operating environment for said protocol processing stack for trusted computing needs of one or more of said networked systems by providing a policy driver for setting up the second hardware processor for a first set of security policy rules to be enforced by said second hardware processor, and a central manager for compiling and distributing said rules of the first set and monitoring the enforcement of said rules of the first set by said second hardware processor, wherein said central manager is configured to provide a second set of security policy rules to said first hardware processor, wherein the rules within the second set are different than the rules within the first set."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 27. For example, Bruton, III et al. do not describe or suggest the distributed network security systems providing a secure operating environment for the protocol processing stack for trusted computing needs of one or more of the networked systems by providing a policy driver for setting up the second hardware processor for a first set of security policy rules to be enforced by the second hardware processor, and a central manager for compiling and distributing the rules of the first set and monitoring the enforcement of the rules of the first set by the second hardware processor, wherein the central manager is configured to provide a second set of

security policy rules to the first hardware processor, wherein the rules within the second set are different than the rules within the first set. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest the distributed network security systems providing a policy driver for setting up the second hardware processor for a first set of security policy rules to be enforced by the second hardware processor, and a central manager that is configured to provide a second set of security policy rules to the first hardware processor, wherein the rules within the second set are different than the rules within the first set. For the reasons set forth above, Claim 27 is submitted to be patentable over Bruton, III et al.

Claim 28 recites a network system comprising "a network comprising a plurality of distributed security systems and one or more networked systems of one or more types, said distributed security systems providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor and said distributed security systems comprise a hardware processor offloading overhead of transport layer protocol processing from said at least one host processor, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said hardware processor comprising a protocol processing engine to do transport layer protocol processing."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 28. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from said at least one host processor. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton,

III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from said at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from said at least one host processor. For the reasons set forth above, Claim 28 is submitted to be patentable over Bruton, III et al.

Claims 29, 30, and 33 depend from independent Claim 28. When the recitations of Claims 29, 30, and 33 are considered in combination with the recitations of Claim 28, Applicant submits that Claims 29, 30, and 33 are patentable over Bruton, III et al.

Claim 31 recites a security system comprising "a storage area network comprising a hardware processor providing transport layer protocol processing, said hardware processor comprising a protocol processing engine for performing transport layer protocol processing; said security system providing multiple protocol layer security in said storage area network."

Bruton, III et al. do not describe or suggest a security system as recited in Claim 31. For example, Bruton, III et al. do not describe or suggest a storage area network comprising a hardware processor providing transport layer protocol processing, the hardware processor comprising a protocol processing engine for performing transport layer protocol processing, the security system providing multiple protocol layer security in the storage area network. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton,

III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a storage area network. For the reasons set forth above, Claim 31 is submitted to be patentable over Bruton, III et al.

Claims 32, 39, and 61 depend from independent Claim 31. When the recitations of Claims 32, 39, and 61 are considered in combination with the recitations of Claim 31, Applicant submits that Claims 32, 39, and 61 are patentable over Bruton, III et al.

Claims 35-38 depend from independent Claim 34, which is recited above.

Bruton, III et al. do not describe or suggest a security system as recited in Claim 34. For example, Bruton, III et al. do not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor providing a remote direct memory access (RDMA) capability and configured to execute a transport layer protocol. For the reasons set forth above, Claim 34 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 35-38 are considered in combination with the recitations of Claim 34, Applicant submits that Claims 35-38 are patentable over Bruton, III et al.

Claims 41-44 depend from independent Claim 40, which is recited above.

Bruton, III et al. do not describe or suggest a security system as recited in Claim 40. For example, Bruton, III et al. do not describe or suggest an RDMA processor configured to execute a plurality of RDMA data transfers and configured to

execute a transport layer protocol. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest an RDMA processor configured to execute a plurality of RDMA data transfers and configured to execute a transport layer protocol. For the reasons set forth above, Claim 40 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 41-44 are considered in combination with the recitations of Claim 40, Applicant submits that Claims 41-44 are patentable over Bruton, III et al.

Claims 46-49 depend from independent Claim 45, which is recited above.

Bruton, III et al. do not describe or suggest a security system as recited in Claim 45. For example, Bruton, III et al. do not describe or suggest a storage area network comprising a remote direct memory access (RDMA) capability for performing RDMA data transfers, the security system providing multiple protocol layer security in the storage area network. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a storage area network. For the reasons set forth above, Claim 45 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 46-49 are considered in combination with the recitations of Claim 45, Applicant submits that Claims 46-49 are patentable over Bruton, III et al.

Claim 50 recites a network system comprising "a network configured to transport network traffic, wherein said network comprises a plurality of distributed

security systems providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor and said distributed security systems comprise a hardware processor offloading overhead of transport layer protocol processing from said at least one host processor, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said hardware processor comprising: a protocol processing engine to do transport layer protocol processing; and a programmable rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 50. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. For the reasons set forth above, Claim 50 is submitted to be patentable over Bruton, III et al.

Claim 51 recites a network system comprising "a network configured to transport network traffic, wherein said network comprises a plurality of distributed security systems providing multiple protocol layer security, wherein each of said distributed security systems comprise at least one host processor, and said distributed security systems comprise a hardware processor offloading overhead of transport layer protocol processing from said at least one host processor, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said hardware processor comprising: a protocol processing engine for performing transport layer protocol processing; a programmable rule-matching engine for analyzing the network traffic for security rule matching or taking actions on matched security rules; and an authentication engine to do encryption, decryption, authorization or authentication using standard or proprietary security protocols."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 51. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of transport layer protocol processing from the at least

one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. For the reasons set forth above, Claim 51 is submitted to be patentable over Bruton, III et al.

Claim 52 recites a security system comprising "a storage area network comprising a hardware processor providing transport layer protocol processing, said hardware processor comprising a storage protocol processing engine for performing storage protocol processing, said security system providing multiple protocol layer security in said storage area network."

Bruton, III et al. do not describe or suggest a security system as recited in Claim 52. For example, Bruton, III et al. do not describe or suggest a storage area network comprising a hardware processor providing transport layer protocol processing, the hardware processor comprising a storage protocol processing engine for performing storage protocol processing, the security system providing multiple protocol layer security in the storage area network. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a storage area network. For the reasons set forth above, Claim 52 is submitted to be patentable over Bruton, III et al.

Claims 53 and 54 depend from independent Claim 52. When the recitations of Claims 53 and 54 are considered in combination with the recitations of Claim 52, Applicant submits that Claims 53 and 54 are patentable over Bruton, III et al.

Applicant respectfully traverses a statement on page 6 of the Office Action. The statement states that in Claims 2, 31, and 52, there are multiple servers 400a, 400b, and 400c detecting intrusions including encryption, decryption between the servers. The statement further states that a network including the servers 400a, 400b, and 400c makes a storage area network. Applicant respectfully submits that Bruton,

III et al. does not disclose or suggest storage and hence, does not disclose or suggest a storage area network.

Claims 56 and 57 depend from independent Claim 55, which is recited above.

Bruton, III et al. do not describe or suggest a security system as recited in Claim 55. For example, Bruton, III et al. do not describe or suggest the hardware processor comprising an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest the hardware processor comprising an RDMA mechanism for performing RDMA data transfer and a protocol processing engine for performing transport layer protocol processing. For the reasons set forth above, Claim 55 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 56 and 57 are considered in combination with the recitations of Claim 55, Applicant submits that Claims 56 and 57 are patentable over Bruton, III et al.

Claims 59 and 60 depend from independent Claim 58, which recites a security system comprising "a storage area network comprising a hardware processor providing a remote direct memory access (RDMA) capability, said hardware processor comprising an RDMA mechanism for performing RDMA data transfer, said security system providing multiple protocol layer security in said storage area network."

Bruton, III et al. do not describe or suggest a security system as recited in Claim 58. For example, Bruton, III et al. do not describe or suggest a storage area network comprising a hardware processor providing a remote direct memory access (RDMA) capability, the hardware processor comprising an RDMA mechanism for performing RDMA data transfer, the security system providing multiple protocol

layer security in the storage area network. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions. Accordingly, Bruton, III et al. do not describe or suggest a storage area network. For the reasons set forth above, Claim 58 is submitted to be patentable over Bruton, III et al.

When the recitations of Claims 59 and 60 are considered in combination with the recitations of Claim 58, Applicant submits that Claims 59 and 60 are patentable over Bruton, III et al.

Claim 62 recites a network system comprising "a network further comprising a plurality of distributed security systems and at least one network system, wherein each of said distributed security systems comprises at least one host processor and said distributed security systems comprise a hardware processor offloading overhead of at least one of a transport layer protocol processing stack and a network layer protocol processing stack from said at least one host processor, wherein said hardware processor is other than said at least one host processor and is configured to receive a command from said at least one host processor, said distributed security systems providing a secure operating environment for said protocol processing stack for trusted computing needs of said at least one network system and said distributed network security systems providing multiple protocol layer security in said network."

Bruton, III et al. do not describe or suggest a network system as recited in Claim 62. For example, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of at least one of a transport layer protocol processing stack and a network layer protocol processing stack from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Rather, Bruton, III et al. describe a host that is depicted as taking responsibility for its own intrusion detection. Bruton, III et al. further describe a sniffer that is continued to be placed in front of the host in some situations. Bruton, III et al. further describe a system that includes a Transmission Control Protocol (TCP) layer that includes a plurality of TCP layer Intrusion Detection System (IDS) functions.

A description of the host that takes responsibility for its own intrusion detection, the sniffer that may be continued to be placed in front of the host, and the system that includes a plurality of TCP IDS functions does not describe or suggest a hardware processor offloading overhead of at least one of a transport layer protocol processing stack and a network layer protocol processing stack from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. Accordingly, Bruton, III et al. do not describe or suggest a hardware processor offloading overhead of at least one of a transport layer protocol processing stack and a network layer protocol processing stack from the at least one host processor, wherein the hardware processor is other than the at least one host processor and is configured to receive a command from the at least one host processor. For the reasons set forth above, Claim 62 is submitted to be patentable over Bruton, III et al.

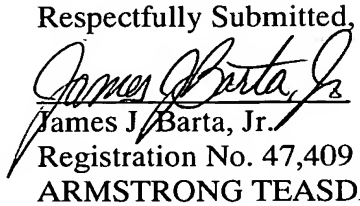
For at least the reasons set forth above, Applicant respectfully requests that the Section 102 rejection of Claims 1-9 and 11-62 be withdrawn.

Newly added Claim 63 depends from independent Claim 1, which is submitted to be in condition for allowance and is patentable over the cited art. For at least the reasons set forth above, Applicant respectfully submits that Claim 63 is also patentable over the cited art.

Newly added Claim 64 depends from independent Claim 2, which is submitted to be in condition for allowance and is patentable over the cited art. For at least the reasons set forth above, Applicant respectfully submits that Claim 64 is also patentable over the cited art.

In view of the foregoing amendment and remarks, all the claims now active in this application are believed to be in condition for allowance. Reconsideration and favorable action is respectfully solicited.

Respectfully Submitted,



James J. Barta, Jr.
Registration No. 47,409
ARMSTRONG TEASDALE LLP
One Metropolitan Square, Suite 2600
St. Louis, Missouri 63102-2740
(314) 621-5070

JJB/NVP/ls